



Department of Defense DIRECTIVE

NUMBER 8570.1

August 15, 2004

ASD(NII)/DoD CIO

SUBJECT: Information Assurance Training, Certification, and Workforce Management

References: (a) [DoD Directive 8500.1](#), "Information Assurance," October 24, 2002
(b) [DoD Instruction 8500.2](#), "Information Assurance (IA) Implementation," February 6, 2003
(c) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001
(d) Section 3544 of title 44, United States Code
(e) through (h), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities, according to references (a) through (d) for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.

1.2. Authorizes the publication of DoD 8570.1-M consistent with reference (e).

2. APPLICABILITY AND SCOPE

This Directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the Department of Defense Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. Contracts for personnel providing IA functional services for DoD information systems (IS) via appropriate Defense Federal Acquisition Regulation Supplement (DFARS) clauses.

3. DEFINITIONS

Terms used in this Directive are defined in references (a) through (c) and/or enclosure 2.

4. POLICY

It is DoD policy that:

4.1. All authorized users of DoD IS shall receive initial IA awareness orientation as a condition of access and thereafter must complete annual IA refresher awareness.

4.2. Privileged users and IA managers shall be fully qualified per reference (b), trained, and certified to DoD baseline requirements to perform their IA duties.

4.3. Personnel performing IA privileged user or management functions, regardless of job series or military specialty, shall be appropriately identified in the DoD Component personnel databases.

4.4. All IA personnel shall be identified, tracked, and managed so that IA positions are staffed with personnel trained and certified by category, level, and function.

4.5. All positions involved in the performance of IA functions shall be identified in appropriate manpower databases by category and level.

4.6. The status of the DoD Component IA certification and training shall be monitored and reported as an element of mission readiness and as a management review item per reference (b).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) shall:

5.1.1. Develop and promulgate additional guidance relating to IA training, certification, and workforce management requirements.

5.1.2. Coordinate the integration of IA initiatives with other workforce development and sustainment requirements.

5.1.3. Establish metrics to monitor and validate compliance with this Directive as an element of mission readiness.

5.1.4. Provide recommended changes to the DFARS to reflect the requirements of this Directive relating to contracts and contractors.

5.2. The Director, Defense Information Systems Agency (DISA) under the authority, direction, and control of the ASD(NII)/DoD CIO shall provide:

5.2.1. Web-based access to current IA policies, techniques, requirements and knowledge resources to support life-cycle enhancement of IA workforce functional competencies.

5.2.2. Baseline training and awareness materials, content, and products on DoD IA policies, concepts, procedures, tools, techniques, and systems for the DoD Components to integrate into their IA training and awareness programs.

5.2.3. Baseline IA training, certification, and tracking program for Designated Approving Authorities (DAA).

5.2.4. In coordination with the Director, National Security Agency a training and certification program for personnel performing Computer Network Defense (CND) Service Provider functions established in reference (c).

5.3. The Under Secretary of Defense for Acquisition, Technology, and Logistics shall:

5.3.1. Provide appropriate IA training for the Defense Acquisition Workforce Improvement Act community.

5.3.2. Coordinate with the DoD CIO to develop clauses in the DFARS to reflect the requirements of this Directive relating to contracts and contractors.

5.4. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) shall:

5.4.1. Establish oversight for approval and coordination of certification development and implementation.

5.4.2. Require that personnel and manpower databases under USD(P&R) authority capture and report requirements for IA training and certification.

5.4.3. Require the Heads of the DoD Components and the Commanders of the Combatant Commands to determine requirements for military and civilian manpower and contract support for privileged users and IA managers based on operational mission support and force structure.

5.5. The Under Secretary of Defense for Intelligence (USD(I)) shall work closely with the ASD(NII)/DoD CIO on IA matters and as necessary:

5.5.1. Require the Director, Defense Intelligence Agency, under the authority, direction and control of the USD(I), to implement this Directive for authorized privileged users and IA managers of DoD non-cryptologic Sensitive Compartmented Information systems and DoD Intelligence Information Systems.

5.5.2. Require the Director, Defense Security Service, under the authority, direction, and control of the USD(I), to incorporate DoD IA awareness products into industrial security programs, as applicable.

5.5.3. Require the Director, National Security Agency, under the authority, direction, and control of the USD (I) to:

5.5.3.1. Implement this Directive for authorized privileged users and IA managers of DoD cryptologic information systems.

5.5.3.2. Implement, in coordination with the ASD(NII)/DoD CIO and the DoD Components, as appropriate, a certification program for Red Teams and Vulnerability Assessments Teams.

5.5.3.3. Establish, in coordination with the DISA, and under the direction of the ASD(NII)/DoD CIO, a training and certification program for personnel performing Special Enclave CND Service Provider functions.

5.6. The Inspector General of the Department of Defense shall provide appropriate IA training for the Inspector General Inspection Team.

5.7. The Assistant Secretary of Defense for Public Affairs shall provide appropriate IA training for public affairs staff and officers.

5.8. The Chairman of the Joint Chiefs of Staff shall:

5.8.1. Develop, coordinate, and promulgate joint doctrine and IA training policies for DoD Joint and Combined operations.

5.8.2. Identify, document, and track in the Joint Manpower and Personnel System all positions and personnel performing any IA functions.

5.9. The Heads of the DoD Components shall:

5.9.1. Establish, resource, and implement IA training and certification programs for all DoD Component personnel in accordance with this policy and references (a), (b), and (c). These programs shall train, educate, certify, and professionalize personnel commensurate with their responsibilities to develop, use, operate, administer, maintain, defend, and retire DoD IS.

5.9.2. Provide initial IA awareness orientation and annual IA refresher awareness to authorized users.

5.9.3. Identify, document, and track IA personnel certifications and certification status in Component personnel databases.

5.9.4. Identify military IA billets in manpower databases based on operational mission support and force structure requirements.

5.9.5. Use the existing abbreviation for Security, "INFOSEC," established in the Office of Personnel and Management (OPM) GS-2210 series (reference (g)) to support DoD-wide civilian IA workforce identification and management requirements. The DoD Components shall ensure that all DoD civilian positions and personnel regardless of OPM series or job title, with IA functions shall use "INFOSEC" as the Position Specialty Code (PSC) in the Defense Civilian Personnel Data System.

5.9.6. Require contracts that include the acquisition of DoD IS IA services to specify certification requirements. Contractor personnel performing IA functions shall have their IA certification category and level documented in the Defense Eligibility Enrollment Reporting System.

5.9.7. Identify, document, track, and report to the DoD CIO the certifications and certification status of all contractors performing privileged user or IA manager functions.

5.9.8. Require all DAAs to be certified.

5.9.9. Provide appropriate IA training for personnel required to enforce DoD IA requirements per this policy and the references.

5.9.10. Provide CND training to CND staffs.


5.9.11. Include IA awareness training and education, as appropriate, in professional military education at all levels.

5.9.12. Capture and report the costs of IA training and certification of personnel, as required by reference (d).

5.9.13. Encourage the use of the Information Assurance Scholarship Program to recruit, develop, and retain DoD IA personnel, as authorized by reference (f).

6. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2

E1. References, continued

E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

- (e) [DoD 5025.1-M](#), "DoD Directives System Procedures," March 5, 2003
- (f) Section 922, National Defense Authorization Act of 2001 (Public Law 106-398)
- (g) Office of Personnel Management Job (OPM) Family Position Classification Standard for Administrative Work in the Information Technology Group, GS-2200; Information Technology Management GS-2210, May 2001, revised August 2003¹
- (h) Chapter 51 of title 5, United States Code

¹ This document can be located at the following Web address: <http://www.opm.gov/fedclass/2200a/gs2200a.pdf>

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Authorized User. Any appropriately cleared individual with a requirement to access a DoD IS for performing or assisting in a lawful and authorized governmental function.

E2.1.2. Categories, Levels, and Functions. The structure for identifying all DoD IA positions and personnel.

E2.1.2.1. Categories. The DoD IA workforce is split into two major categories of Technical and Management. IA manager refers to personnel performing any IA management function.

E2.1.2.2. Levels. Each of the IA workforce categories has three levels (Technical or Management Level 1, 2, and 3). The management category also includes the DAA position.

E2.1.2.3. Functions. The specific IA job requirements associated with a category and level. The functions provide a means to distinguish between different levels of work. The functional level indicates the roles that an employee performs or occupational requirements to successfully perform at different levels of the IA Workforce. The functional level approach also encourages a broader, more integrated means of identifying what an employee must know to perform the tasks that comprise an IA position across all of the DoD Components.

E2.1.3. Certification. Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or profession. Certification provides verification of individuals' knowledge and experience through evaluation and approval based on a set of standards for specific profession or occupations' functional job levels. Each certification is designed to stand on its own, and represents a certified individual's mastery of a particular set of knowledge and skills.

E2.1.4. Defense Civilian Personnel Data System (DCPDS). The DCPDS is a human resources transaction and information system that supports civilian personnel operations in the Department of Defense. The DCPDS is designed to support appropriated fund, nonappropriated fund, and local national human resources operations. DCPDS data elements shall be used to document and track civilian personnel information in support of requirements of this Directive.

E2.1.5. DoD Information System (IS). A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. This includes automated information system applications, enclaves, outsourced Information Technology (IT)-based processes, and platform IT interconnections per reference (b).

E2.1.6. Local National Personnel. Civilian personnel, whether paid from appropriated or nonappropriated funds, employed or utilized by U.S. Forces in a foreign country who are nationals or non-U.S. citizen residents of that country.

E2.1.7. General Schedule (GS)/Pay Band. The basic classification and compensation system for white-collar occupations in the Federal Government, as established by Chapter 51 of title 5, U.S.C. (reference (h)).

E2.1.7.1. Job Series: A subgroup of an occupational group or job family that includes all classes of positions at the various levels in a particular kind of work, such as the 2210 series. Positions within a series are similar to each other with regard to subject matter and basic knowledge and skill requirements.

E2.1.7.2. Position Specialty Code (PSC): This is a unique DoD civilian workforce code to support effective management of the IA workforce. The PSC identifies a DoD civilian position or person with IA functions regardless of OPM job title.

E2.1.8. Privileged User. An authorized user who has access to system control, monitoring, administration, criminal investigation, or compliance functions.

E2.1.9. Red Team. An independent and focused threat-based effort by an interdisciplinary, simulated adversary to expose and exploit vulnerabilities to improve the security posture of IS.

E2.1.10. System Administrator. Individual responsible for the installation and maintenance of an IS, providing effective IS utilization, adequate security parameters, and sound implementation of established IA policy and procedures.

E2.1.11. Training

E2.1.11.1. Resident: Instructor-led in-class instruction.

E2.1.11.2. Distributive: Computer-based training via web site, computer disk, or other electronic media.

E2.1.11.3. Blended: A combination of instructor-led and distributive media. This may also include instructor-led via distributive multi-media.

E2.1.11.4. On the Job Training: Supervised hands-on training, based on specific performance criteria that must be demonstrated to a qualified supervisor.

E2.1.12. Vulnerability Assessment Team. A team of highly skilled individuals who conduct systematic examinations of IS or products to determine adequacy of security measures, to identify security deficiencies, to predict effectiveness of proposed security measures, and to confirm adequacy of such measures after implementation.